REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10-30-2014	FINAL	

4. TITLE AND SUBTITLE

Life, Liberty, the Pursuit of Happiness?:
Cyberhate, Cybercrime, and Cyberterrorism in Burma

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LtCol Randolph G. Pugh, USMC

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Recent governmental reform in Burma is precipitating calls to remove longstanding restraints on people's activity on the Internet. While many people in Burma would benefit from fewer controls, there are some who would use this freedom to cause internal strife, commit cybercrime, and conduct cyberterrorism. Burma faces a real dilemma: implementing strict Internet controls will lead to accusations that the government is continuing censorship and human rights abuses but insufficient monitoring and regulation will allow criminals and terrorists to "end run" existing physical controls and give a hateful few a new way to spread discontent. For this reason, the U.S. Government should support and assist the Burmese government as it takes a disciplined and measured approach to Internet adoption in order to preserve regional stability, enhance global security, and prevent unnecessary suffering by the Burmese people.

15. SUBJECT TERMS

Burma, Myanmar, Internet, Information Communications Technology, Cyberhate, Cybercrime, Cyberterrorism

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		25	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

LIFE, LIBERTY, AND THE PURSUIT OF HAPPINESS?: CYBERHATE, CYBERCRIME, AND CYBERTERRORISM IN BURMA

by

Randolph G. Pugh

Lieutenant Colonel, United States Marine Corps

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

30 October 2014

Contents

Paper Abstract

Recent governmental reform in Burma is precipitating calls from inside and outside of the country to remove longstanding constraints on people's activity on the Internet. The ability to communicate one's thoughts globally and openly without restriction seems the pinnacle of liberalism and certainly something the United States should support. This assumes universal benevolent intent, however. The Internet, and the connectivity to people and information it provides, is neither good nor bad. While many good people in Burma would benefit from increased access and fewer controls, there are also some who would use this freedom to cause internal strife, commit cybercrime, and conduct cyberterrorism.

Burma faces a real dilemma. On one hand, implementing strict Internet controls will lead to accusations that the government is continuing with old *junta* practices of censorship and human rights abuses. On the other, insufficient monitoring and regulation by the Burmese government will allow criminals and terrorists to "end run" existing physical controls and a hateful few the opportunity to entice the population into attacking their own countrymen. The United States has a vested interest in a stable Burma and human rights and should therefore support and assist the Burmese government as it balances Internet freedoms with necessary controls on cyberhate, cybercrime, and cyberterrorism.

Introduction

In 2010, few inside or outside of Burma expected much change following national elections that observers roundly criticized as flawed.[1] Thein Sein, the newly-elected president, had served as the country's Prime Minister since 2007. Members of the recently-dissolved military *junta* also did well, winning 80 percent of the parliamentary seats.[2] Thein Sein insisted, however, that he would make sweeping changes to the government, stating in an early BBC interview that he was "merely responding to the people's desire for reform" and that "[his] future depends on the people and their wishes."[3] He would have plenty to fix in the area of telecommunications. In 2010, Burma was one of the most isolated states on the planet with an estimated 7 televisions and 107 landline telephones per 1,000 citizens.[4] Only one person in a hundred owned a cell phone and one in five hundred had an Internet connection.[5] Just 10% of the population had a radio with which to listen to one of the four government-owned radio stations.[6] Burma's telecommunications policies, state censorship, and legal and extralegal restrictions on the population's freedom of expression led Reporters Without Borders to rank Burma 173 of 178 countries on the Press Freedom Index and to label its government "an enemy of the Internet."[7]

President Thein, however, has proved to be a surprisingly progressive moderate and has, since his election, achieved impressive progress toward making Burma a fully-functional member of the international community. As will be detailed in this paper, one area where he has largely kept his promises is in the area of telecommunications. He has loosened, if not completely removed, fifty years of stifling practices and policies. Through increased social and political liberalization, turbo-charged with massive foreign investment possible

following the relaxation of international sanctions, he is poised to bring the majority of Burmese people to the global Internet community-and vice versa.

The United States, as one would expect, enthusiastically supports the ubiquitous global interconnectedness and the associated empowerment of the individual the Internet will bring to Burma. The Internet, however, empowers both creation and destruction equally. Its introduction to a society, especially one experiencing a concurrent social, political, and technical revolution, requires careful control. Unsurprisingly, since 2012, modest increases in connectivity and some relaxations on Internet use have already caused issues for the Burmese government and for the Burmese people. The massive explosion of Internet availability Burma will experience in the next two years, and the associated connection of the population to the rest of the world, has the potential to radically increase intolerance, crime, and terrorism in Burma, in Southeast Asia, and around the world. For this reason, the United States government should support and assist the Burmese government as it takes a disciplined and measured approach to Internet adoption in order to preserve regional stability, enhance global security, and prevent unnecessary suffering by the Burmese people.

The Coming Telecom Revolution in Burma

The growth of the telecommunications industry over the next three years in Burma, and the corresponding ability for the Burmese population to communicate, promises to be truly revolutionary. In 2011, Burma ranked next to last in mobile phone penetration rates, behind even notoriously reclusive North Korea, with less than 1% of the population owning a mobile device.[8] Internet availability was similarly anemic with a measly .2% of the population online and those users severely limited by government-controlled content filtering and their activities subject to arrest and imprisonment under the heavy-handed Electronic

Transaction Law.[9] Through a combination of limiting availability and restricting activities, the Burmese government had consciously and effectively isolated its entire population from external and internal digital dissent.

In 2011, as part of a large-scale modernization effort, the Burmese government began to breathe life into the telecommunications sector. One initial measure was correcting the cost for SIM cards to access the government-owned, antiquated cellular network. In 2011 the cards cost $625, well outside the reach of all but a handful of Burmese citizens.[10] By 2013 a new policy mandated $250 as the maximum price for a SIM card.[11] Mobile phones suddenly became more affordable for the small Burmese middle class and ownership grew 1,125%.[12] A similar phenomenon took place in regards to Internet usage. When the government removed the filters that had made most external Internet sites, certainly those critical of the government, unreachable for years and granted blanket amnesty to bloggers who had been imprisoned for violations of the Electronics Transactions Law, young Burmese began to frequent Internet cafés in increasing numbers and with increasing confidence. The number of Internet users in Burma, largely unchanged from 2006 - 2010, grew 480% from 2011 to 2013.[13] This growth, while impressive, will pale in comparison to what industry experts expect for the period 2014 - 2016.

In 2012, coincident with the loosening of international sanctions, the Burmese government solicited internationally for companies to help it modernize the country's outdated national telecommunications infrastructure. In 2013 it awarded contracts to a Norwegian (NoreTel) and a Qatari (Ooredoo) company. These companies, and two domestic providers, collectively committed to bringing 3G[14] cellular service to 80% of the population by 2016, including coverage to the majority of the rural areas.[15] When service in Yangon,

Madalay, and Naypyidaw premiered in August of 2014, Ooredoo sold out of its estimated three month's supply of $1.50 SIM cards in two days.[16] NoreTel and the two domestic telecoms have launches just behind Ooredoo's and offer similar pricing plans. Assuming neighboring countries are analogous, this combination of low initial investment costs and widespread availability should bring a large number of Burmese citizens onto the 3G network, and thereby onto the Internet, in short order.[17]

The explosion of mobile phone and Internet availability and the corresponding effect it will certainly have on all aspects of society will make Burma one of the most exciting information communications technology (ICT) markets in the world over the next decade. It is not unrealistic that during this time as many as thirty million Burmese, previously physically and informationally isolated within the borders of their country, will join the global online community. International ICT-related companies certainly see an opportunity. In the past year, Cisco, Microsoft, Google, Facebook, PayPal and other companies have sent their corporate leadership to Naypyidaw in an effort to stake their claim to a portion of this digital gold rush.[18] One thing these leaders consistently note as an impediment to progress, a viewpoint shared with many within Burma, is the Burmese government's current ambiguity on the issue of its population's freedom of expression online and suspicions that officials will use the expansion of the Internet to expand their repression of the people.[19] Based on past abuses, many people resent, and even fear, governmental oversight of the Burmese population's actions on the net. While acknowledging excesses of the past and taking a more tolerant view on Internet usage is necessary, Burma is correct in treating very seriously, the dangers lurking in cyberspace.

The Dark Web and Dangers of the Internet

The Internet's ability to enable communications between people around the globe has proved as revolutionary as any other technology in history. In the overwhelming majority of cases, the unrestricted sharing of ideas and information has radically improved work efficiency and has globalized industry and marketplaces. It has enabled education and other transfers of knowledge and exposed people to new concepts, art, and music they would never have the opportunity to experience in person. With just a simple connection to the net, all of this is possible regardless of a user's physical location, age, social status, race, gender, religious belief, or wealth. There is another side of the Internet, one that also does not discriminate, however.

As the Internet is merely a conduit for information, it efficiently and effectively enables virtuous and nefarious behavior equally. Some illegal or immoral activities take place on the "surface web," that part of the Internet indexed and able to be queried by search engines and easily discovered by normal users. Examples include inflammatory language on Facebook, false or misleading websites, or websites that infect the visitor's computer with malicious code. The worst activities, however, take place on the "deep web" or "dark net." The deep web is the portion of the Internet hidden from casual users, and in most cases, all law enforcement. This is where illicit users use untraceable bitcoins to buy illegal drugs and guns off the Silk Road[20], conduct human trafficking, buy false passports, or trade in stolen credit card numbers. Users can even find advertisements for assassination services and weapons of mass destruction.[21] Considering the meteoric rise of the Internet in Burma, millions of Burmese will soon be able to buy and sell physical objects and to trade ideas and information on both the surface web and the deep web.

Cyberhate

One considerable danger for a country filled with large numbers of naïve Internet users, and in a country where the population has no historical context for freedom of speech, is the use of the Internet by one portion of the population to incite hate or violence against another. One Burmese issue especially vulnerable to this kind of online inflammation is the ongoing conflict between Buddhist Rakhine and the Muslim-minority Rohingya. In fact, it is already taking place. In 2012, anti-Rohingya rhetoric, insults, accusations, and calls to action on the Internet turned into physical violence in western Burma. The ensuing riots resulted in eleven mosques burned, 250 Rohingya murdered, and a further estimated 140,000 displaced from their homes.[22] In 2014, the Internet provided the Buddhist monk Ashin Wirathu, self-proclaimed as "the Burmese Bin Laden," a new means to stoke the fire of religious-nationalistic violence. A single post on his Facebook page that a Buddhist girl had been raped by a Muslim man in Mandalay drew a stone-throwing crowd of over 300 people to the man's tea shop. The subsequent riot and police response resulted in the deaths of two men and the imposition of state-wide martial law.[23] Resentment and anger continues to simmer on both sides, much of it expressed online.

The use of social media has proved exceptionally popular in Burma. For historical and cultural reasons, sites like Facebook effectively "virtualize" how the Burmese have learned to interact socially in the physical world. Facebook also carries a level of credibility not seen in many other countries. After decades of living under tight governmental control, the informal sharing of information has become the normal way of passing news. In this community, as Matthew Schissler from Paung Ku, a Burmese civil society strengthening organization, explains it, "rumor and word-of-mouth information are more credible than the

news and government announcements in a place where censorship and propaganda have long been the norm."[24] This instinctive trust, combined with the ease of misattribution of sources and falsification of images or information made possible by the Internet, makes a dangerous combination. Beyond lending unwarranted credence to accusations, cyberspace also now allows hate speech to reach a global audience instantaneously.

Surprisingly, the only thing that the Burmese fear more than an uncontrolled ethno-religious crisis inflamed by the hate speech of bloggers, Facebook posters, and Tweeters is the sudden reappearance of oppressive government censorship and criminalization of online expression. In the words of Nay Phone Latt, a blogger who was imprisoned for four years under still-current laws prohibiting criticism of the government, "if we don't regulate ourselves… they will take the power back."[25] He has a valid concern. While the government has not acted on it during the current period of transition, the 2004 Electronic Transactions Act has never been rescinded.[26] In this legal uncertainty the Burmese government and its population struggle to find the delicate balance between privacy, freedom of speech, security, and stability.

Cybercrime

Controlling crime, including transnational crime, has always been a challenge for the Burmese government. For example, in 1989 the government ceded a large part of the northeast of the country to the United Wa State Army (UWSA) after the ethnic minority group fought the military to a cease fire and gained autonomy within the Shan state. The UWSA has been called "the world's largest narcotics organization."[27] The area they control is Burma's portion of the infamous "Golden Triangle," an area second only to Afghanistan for opium production.[28] Along with methamphetamine and heroin, the value of the illicit

drug trade from this region is estimated at between one and two billion dollars per year.[29] Crime also pervades the rest of the country in the form of human trafficking, weapons smuggling, trade in endangered species, and money laundering.[30] Decades of corruption within the ruling *junta* not only allowed this criminal activity to take place but also, in many cases, supported it for personal profit. The Congressional Report on Crime in Burma effectively sums the situation up in its opening statement: "transnational organized criminal groups flourish in Burma."[31] With all of its problems controlling the physical aspects of crime, the introduction of widespread Internet availability, with its intrinsic lack of regulation, will assuredly create additional challenges for the government.

In its simplest form cybercrime is simply a virtual manifestation of a physical crime or criminal transaction. It consists of stealing physical things, intellectual property, or money. It can also involve trafficking illegal goods or people, providing illegal services, or committing fraud. Widespread Internet availability in Burma will simply increase the number of potential vendors for illegal products and services as well as the number of potential customers. It will globalize Burma's booming illegal marketplace. It will also increase the number of potential victims. Fifty years of relative isolation has left a citizenry that is just beginning to experience networked technologies commonplace elsewhere in the world. For example, with the exception of a few hotels in Yangon, credit cards are not accepted in Burma and ATMs are just beginning to appear, but only in major tourist areas heavily frequented by Westerners.[32] Criminals, adept at leveraging the Internet to their advantage, will find a newly-connected Burma a lucrative environment. At least initially, there is no expectation that the Burmese citizens will have much savviness about protecting themselves from these cybercriminals.

Another target for attack by cybercriminals worldwide will be the millions of new computers connected to the Internet in Burma. Criminal organizations gain anonymity and complicate local and international law enforcement by "hijacking" computers in other countries. In 2011, even a relatively disconnected Burma suffered these types of attacks. In the first quarter of that year, Burma led the world with 13% of all malicious Internet traffic.[33] This traffic, the report acknowledged, was most likely not Burmese hackers but rather simply Burma-based computers providing a launch point for criminals residing elsewhere. Vietnam also experiences this kind of exploitation. Microsoft recently named Vietnam one of the largest victims of cybercrime in the world.[34] Widespread vulnerability, attributed to the population's poor understanding of effective security practices, sharing of pirated software, and general naïveté regarding privacy, allowed cybercriminals to infect nearly 50% of the computers in the country with malicious code.[35] The costs for Vietnam, as they will be for Burma, are both direct, when theft in Vietnam occurs, and indirect, as Vietnam must pay for workers' lost productivity and the excessive bandwidth used by its "zombie" computers.

The phenomenon of cybercrime will likely evolve in Burma over time. As Burma's citizens come online, the majority of cybercrime will likely be of the simplistic form — crime by individuals affecting individuals. As the country networks government organizations and the commercial sector over time, though, these targets will become the preferred target of cybercriminals. Without adequate technical, legal, and policy controls in place, Burma's Internet revolution risks failing to enable the economy or the population to its full potential. This is certainly not Thein Sein's desire, nor that of the United States.

Cyberterrorism

One more tremendous challenge for Burma will be the conduit that the Internet will provide between terrorist organizations and the Burmese people. In a global context, the ongoing Rohingya crisis provides exactly the kind of grievances that attract the attention of international terrorist organizations. In fact, in August 2014, Al Qaeda's leader, Ayman al-Zawahiri declared the creation of Al Qaeda in the Indian Subcontinent, ostensibly to unite the Muslim people of this region. Burma was specifically mentioned in his YouTube announcement video.[36] It appears that along with democratic reforms, transnational terrorism is also coming to Burma.

As cyberterrorism is often misunderstood, it is worth briefly mentioning that the danger to Burma is not that of *cyberwarfare*. Cyberwarfare is the use of the Internet to attack critical infrastructure, the networked portions of governmental or non-governmental institutions, or even the digital infrastructure itself.[37] Most countries, Burma included, are simply too disconnected from the net to make much of a target for a cyberattack. Most terrorist organizations also find planning and executing an effective cyberattack incredibly difficult and not worth the significant investment.[38] The real threat to the Burmese government and population will be terrorist organizations' more routine use of the Internet as a means to raise funds, recruit, spread propaganda, and encourage acts of violence.[39]

Terrorism thrives on the Internet. The low cost to establish a presence, the inherent anonymity, the reach of a global audience, and the difficulties nation-states have in policing cyberspace makes the Internet an unbeatable communication method. A United Nations study conducted in 2004 found that virtually every known terrorist organization had its own website.[40] The widespread connectivity of Burmese society will bring the population into

regular and close contact with terrorists once these sites become just a click away on a mobile phone. The results may be dire: more, better-funded terrorists; increasingly radicalized minority groups within Burma; and terrorist attacks in greater numbers and sophistication. While many terrorists will limit their activities only to Burma, including targeting the Burmese government, others will have regional and global agendas. The substantial ungoverned spaces in Burma, soon with Internet service, may be attractive to terrorist organizations increasingly under pressure elsewhere in the world.

Given the number of already-existing issues and the new grievances sure to result from social, political, and economic reform, terrorism will likely be part of Burma's future. For example, the UWSA's existence is becoming an increasingly embarrassing reminder of the past corruption and criminal complicity of the Burmese government.[41] It is conceivable that funding terrorist attacks outside of the Shan state might be an attractive way to distract the military from any thoughts of attempting to reestablish control of UWSA-held areas and the associated drug trade. Similarly, nationalistic Buddhists desperate to drive the Rohingya out of Burma would likely appreciate the support of individuals and organizations with similar motivations, regardless of where they physically reside. Using the same logic, a real danger exists that 140,000 disenfranchised and displaced Rohingya in the Rakhine state provide a willing pool of recruits for Muslim terrorist organizations offering *jihad* at home or abroad.[42]

The challenge for the Burmese government, as with cyberhate and cybercrime, will be to craft policies, laws, and impose technical oversight that preserves security and stability while respecting the newly rediscovered rights of its citizens: freedom of speech, privacy, and a freedom from unreasonable content filtering. The challenge is tremendous. Beyond

tackling the process of identifying, pursuing, arresting, and prosecuting terrorists, Burma will first have to define what it considers a "terrorist," a nontrivial task. The Burmese government should expect that terrorists will challenge any controls of online behavior as they relentlessly press their online recruiting, fundraising, and proselytizing. They will also use a tactic in the virtual world that they use extensively in the physical world. Any overreaction by the government to cyberterrorists methods, either through policy or police crackdown, will be highlighted and magnified as a method to drive a wedge between the government and its people — with grave consequences for both.

Recommendations

The United States is in a unique position to assist the Government of Myanmar as it struggles with the numerous issues certain to arise during its period of explosive Internet growth. While the natural tendency is to distrust the Burmese government after fifty years of oppression of their population, it is in America's interest to help. This will not be politically easy. Beyond the distaste of working with former *junta* members, assisting another country in monitoring and controlling their citizen's online activity so close on the heels of accusations against the U.S. National Security Agency of spying on its own citizens, may confuse our allies in Asia, elsewhere in the world, and even our own citizens. There are risks, however, to doing nothing.

As Internet adoption becomes widespread in Burma, the Burmese government may assume a *laissez-faire* attitude toward policing the Internet. Cybercriminals and cyberterrorists will take advantage of this tremendous opportunity and will exploit the Burmese people, foreign investors, tourists, and even the government itself. Factions within Burma may also see this newfound freedom as an opportunity to settle old scores resulting in

destabilization of the country due to ethno-religious violence. A second possible outcome is that, based on initial difficulties, Burma's government decides that Internet freedom risks are simply not worth the gains. The resumption of censorship, restrictions on free speech, and prosecution of online dissent would be catastrophic for the country's population and would turn Burma into an impossible partner for the United States.

Technical Assistance

The United States can assist in Burma with implementing technical measures appropriate to secure the country's infrastructure and population from cybercriminals and cyberterrorists. The recent stand-up of the U.S. Cyber Command provides a center of excellence within the Department of Defense for analyzing an adversary's computer exploitation techniques and technologies and then developing methods for protecting networks. Other federal agencies have similar cyber expertise appropriate to their domains (e.g. Department of the Treasury, Department of Justice, Federal Communications Commission). An interagency approach to engagement might be invaluable to the Burmese government as they attempt to map a disciplined evolution to a networked society.

Depending on the United States government's and Burmese government's unwillingness to work bilaterally on the sensitive topic of telecommunications infrastructure security, there might need to be other ways with which to cooperate less obtrusively. One solution may be via the Association of Southeast Asian States (ASEAN), which has agreements in place to encourage cybersecurity assistance between partner nations.[43] Another potential choice exists in a public-private partnership which supports the United Nations' International Telecommunication Union (ITU) called the International Multilateral Partnership Against Cyber Threats (IMPACT). ITU-IMPACT, built at the urging of the

Malaysian government and headquartered near Kuala Lumpur, is tasked to "provide … Member States access to expertise, facilities and resources to effectively address cyber threats."[44] The United States is neither a member of ASEAN nor ITU-IMPACT. It does, however, regularly share cybersecurity expertise, incident reporting, and conduct cooperative training and exercises with both organizations or their member nations.[45] Cooperation with either ASEAN or ITU-IMPACT effectively provides a conduit for technical assistance to Burma, thereby helping to improve its cybersecurity, and by extension, regional and global cybersecurity.

Freedom of the press, speech, and expression

Regardless of technical solutions to curbing cybercrime, or cyberterrorism, the first and largest issue Burma must solve is the question of how human rights and freedom of expression might be balanced with reasonable online restrictions. Acknowledging that this is a Burmese problem for the Burmese government and people to solve, the United States can assist. America has struggled for over two hundred and thirty-eight years with the freedom of expression versus security paradox and has accumulated significant expertise meeting the challenges of imposing an equitable rule of law on the Internet. The U.S. Constitution's First Amendment, whether in cyberspace or in the physical world, has limits. Current U.S. cyber-related legislation and decades of legal case precedents might provide the Burmese government a sense of how Internet controls might be applied in their country — and applied in a manner that would be held in high regard by the United States and other states with democratic traditions.

As with the issue of technical assistance, close direct cooperation between our governments may be too hard for one or both countries at the present. There are, however,

other organizations that can assist with Burma's struggle to reasonably control the Internet. Burma already has a strong relationship with the United Nation's Office on Drugs and Crime (UNODC),[46] whose mandate has recently expanded to include cybercrime and cyberterrorism.[47] This organization has extensive expertise in assisting member countries with integrating Internet-based activities into existing government paradigms, specifically recommending policies, laws, and surveillance mechanisms that allow freedom of expression and that respect international human rights standards while still detecting illegal behavior, apprehending perpetrators, and prosecuting them under the rule of law.[48] Our support of UNODC, and their subsequent support to Burma, would ensure excellent support to the Burmese government while also lending the country a measure of indisputable international legitimacy which cyberhaters, cybercriminals, cyberterrorists would find difficult to contest.

Grasping the Extended Hand

Lastly, one of the easiest and most effective measures the United States might take is to overtly express support and encouragement to the Burmese government during their struggle to modernize. While a large degree of mistrust still exists between the United States and Burma as well as between Burma's population and its own government, signs of progress are unmistakable. It should be possible to endorse policies we support without a wholesale endorsement the government. Insight into the challenges the Thein government faces in the unique socio-cultural and historical context of Burma might lead to previously-unrealized opportunities for further cooperation. Additionally, with a non-accusatory voice in the conversation, we have the potential to influence Burmese leadership in a way that will make the country a strong partner for regional and global security as well as a robust economic partner. The world is becoming overwhelmingly interdependent. It is appropriate

that the Internet, the catalyst for this interdependence, should be one of the first areas where the United States reengages with Burma.

Conclusion

For nearly fifty years, a corrupt and repressive military regime in Burma represented the antithesis of the American ideals of life, liberty, and the pursuit of happiness. Despite draconian political and economic measures, the United States Government could never pressure the *junta* into discontinuing human rights abuses, curbing illegal activities, reforming the military, adopting more egalitarian economic policies, improving social services, or even simply allowing their people a basic measure of freedom of expression. Thein Sein's election in 2011, however, brought about a new, exciting possibility. As part of a broader effort to democratize the society and capitalize its economy, the Burmese government has made real progress in the modernizing mobile communications, improving access to the Internet, and relaxing long-standing policies prohibiting free speech. In many cases, these changes have surpassed even their own citizens' most optimistic hopes. Sadly, but predictably, some elements inside and outside of Burma now want to take advantage of these loosened controls, the associated challenges they pose to the Burmese government, and the general Internet naïveté of the Burmese people. For practical reasons, the United States now finds itself in the strange position of trying to convince Burma to impose <u>more</u> not less control over the free and open communication that is about to sweep over the country. It is, counterintuitively, restricting what the Burmese people can say or do on the Internet, though, that will best enhance Burma's stability, security, and prosperity and that will give the Burmese people their best chance for happiness.

NOTES

[1] BBC News, "Western States Dismiss Burma's Election," November 8, 2010, http://www.bbc.com/news/world-asia-pacific-11707294.

[2] Humanitarian Information Unit, U.S. Department of State, "Burma 2010 Election Results," accessed October 15, 2014, https://hiu.state.gov/Products/Burma_Elections2010and2012_2012Mar22_HIU_U553.pdf.

[3] BBC News, "Profile: Burma President Thein Sein," October 11, 2012, http://www.bbc.com/news/world-asia-pacific-12358204.

[4] NationMaster, accessed October 20, 2014, http://www.nationmaster.com/country-info/profiles/Burma/Media/All-stats.

[5] Ibid.

[6] Ibid.

[7] Reporters Without Borders, "Press Freedom Index 2010," accessed October 25, 2014, http://en.rsf.org/press-freedom-index-2010,1034.html.

[8] The World Bank, accessed October 11, 2014, http://data.worldbank.org.

[9] Freedom House, "Freedom on the Net 2011," April 18, 2011, http://www.freedomhouse.org, 76-77.

[10] Freedom House, "Freedom on the Net 2013 (Burma)," October 3, 2013, http://www.freedomhouse.org, 6-7.

[11] Ibid., 7.

[12] The World Bank, accessed October 11, 2014, http://data.worldbank.org.

[13] Ibid.

[14] "3G" refers to the third generation of the Global System for Mobile Communications standard. The biggest difference between 2G and 3G is that 2G data rates allow users only voice calls and simple data services (e.g. text messages) while 3G's faster speeds allow full web browsing, sharing of photos, streaming video, voice over Internet protocol (VoIP) telephony, etc.

[15] Chun Han Wong and Shibani Hatani, "Telenor and Qatar Telecom Win Myanmar Licenses," *The Wall Street Journal*, June 27, 2013, http://online.wsj.com/.

[16] Dylan Bushell-Embling, "Ooredoo Launches 3G Services in Myanmar," *Telecom Asia*, August 18, 2014, http://www.telecomasia.net/.

[17] For comparison, Thailand, which has nearly country-wide cellular coverage and an average SIM card price of $5, has an effective mobile phone penetration rate of over 100%. See NationMaster, accessed October 20, 2014, http://www.nationmaster.com/country-info/profiles/Burma/Media/All-stats.

[18] Oxford Business Group, "Myanmar: Internet Conundrum," April 26, 2013, http://www.oxfordbusinessgroup.com/.

[19] Jared Ferrie and Aung Hla Tun, "In the New Myanmar, an Old Junta's Laws Survive and Adapt," Reuters, September 5, 2013, http://www.reuters.com.

[20] The Silk Road was an anonymous online black market run on the deep web by an administrator who called himself "The Dread Pirate Roberts." The majority of the illegal items for sale were drugs as the site's terms of service prohibited any items meant to "harm or defraud." Users needed to look elsewhere for child pornography or weapons of mass destruction. The FBI estimated The Silk Road may have serviced as much as $45 million worth of transactions per year. Dread Pirate Roberts' was arrested by the FBI in March of 2014. One month later "The Silk Road 2.0" appeared on the deep web. See Silk Road Drugs, "Silkroad," accessed October 28, 2014, http://silkroaddrugs.org/silkroad/.

[21] For an excellent primer on the deep web see: Dean Walsh, "A Beginner's Guide to Exploring the Darknet," accessed October 24, 2014, http://electronician.hubpages.com.

[22] Sai Latt, "Intolerance, Islam and the Internet in Burma," New Mandala, June 10, 2012, http://asiapacific.anu.edu.au/newmandala/.

[23] Gianlucca Mezzofiore, "Wirathu's 'Buddhist Woman Raped' Facebook Post Stokes Anti-Muslim Violence in Mandalay," *International Business Times*, July 2, 2014, http://www.ibtimes.co.uk/.

[24] Hereward Holland, "Facebook in Myanmar: Amplifying hate speech?," Al Jazeera, June 14, 2014, http://www.aljazeera.com/.

[25] Ibid.

[26] Freedom House, "Freedom on the Net 2013 (Burma)," October 3, 2013, http://www.freedomhouse.org, 12.

[27] Stratfor Global Intelligence, "Myanmar: The United Wa State Army's Uncertain Future," July 22, 2013, http://www.stratfor.com/.

[28] Congressional Research Service, *CRS Report for Congress: Burma and Transnational Crime*, August 21, 2008, 6.

[29] Ibid., 9.

[30] Ibid., 1-16.

[31] Ibid., 4.

[32] Lonely Planet, "Burma/Myanmar," accessed 15 October 2014, http://www.lonelyplanet.com/myanmar-burma/practical-information/money-costs.

[33] Info Security, "Myanmar Surprises as Top Source of Malicious Internet Traffic," August 10, 2011, http://www.infosecurity-magazine.com/.

[34] Mircrosoft, *Microsoft Security Intelligence Report*, 2014, 50.

[35] Ibid., 121.

[36] Ishaan Tharoor, "Why Al-Qaeda is Opening a New Wing in South Asia," *The Washington Post*, September 3, 2014, http://www.washingtonpost.com.

[37] Gabriel Weimann, "How Modern Terrorism Uses the Internet," U.S. Institute of Peace, March 2004, http://www.usip.org/sites/default/files/sr116.pdf, 2.

[38] Martin Libicki, "Don't Buy the Cyberype: How to Prevent Cyberwars from Becoming Real Ones," *Foreign Affairs*, August 13, 2013.

[39] Weimann, 7 - 9.

[40] Wiemann, 2.

[41] Stratfor Global Intelligence, "Myanmar: The United Wa State Army's Uncertain Future," July 22, 2013, http://www.stratfor.com/.

[42] This already happens in India where some persecuted Muslims are traveling to Syria to fight for the Islamic State. See Saurabh Gupta, "One of the Four Indians Suspected to Have Joined ISIS Reportedly Dead," NDTV, August 27, 2014, http://www.ndtv.com.

[43] Caitríona H. Heinl, "Moving Toward a Resilient ASEAN Cybersecurity Regime," *Asia Policy*, no. 18 (July 2014), http://asiapolicy.nbr.org.

[44] ITU-IMPACT, "Mission," accessed October 26, 2014, http://www.impact-alliance.org/aboutus/mission-&-vision.html.

[45] ITU-IMPACT, *2012 Report*, accessed October 26, 2014, http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf ; U.S. State Department, "U.S. Engagement in the 2014 ASEAN Regional Forum," August 10, 2014, http://www.state.gov/r/pa/prs/ps/2014/230479.htm.

[46] United Nations Office on Drugs and Crime, "Myanmar and UNODC Sign Landmark Agreement to Strengthen the Rule of Law and Counter Crime and Drug Threats," August 18, 2014, https://www.unodc.org/southeastasiaandpacific/en/myanmar.

[47] United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, 2012, http://www.unodc.org/documents/.

[48] Ibid.

BIBLIOGRAPHY

BBC News. "Western States Dismiss Burma's Election." November 8, 2010. http://www.bbc.com/news/world-asia-pacific-11707294.

————-. "Profile: Burma President Thein Sein." October 11, 2012. http://www.bbc.com/news/world-asia-pacific-12358204.

Bushell-Embling, Dylan. "Ooredoo Launches 3G Services in Myanmar." *Telecom* Asia. August 18, 2014. http://www.telecomasia.net/.

Congressional Research Service. *CRS Report for Congress: Burma and Transnational Crime.* August 21, 2008.

Ferrie, Jared and Tun, Aung Hla. "In the New Myanmar, an Old Junta's Laws Survive and Adapt." Reuters. September 5, 2013. http://www.reuters.com.

Freedom House. "Freedom on the Net 2011." April 18, 2011. http://www.freedomhouse.org.

————-. "Freedom on the Net 2013 (Burma)." October 3, 2013. http://www.freedomhouse.org.

Gupta, Saurabh. "One of the Four Indians Suspected to Have Joined ISIS Reportedly Dead." NDTV. August 27, 2014. http://www.ndtv.com.

Heinl, Caitríona H. "Moving Toward a Resilient ASEAN Cybersecurity Regime." *Asia Policy*. no. 18 (July 2014). http://asiapolicy.nbr.org.

Holland, Hereward. "Facebook in Myanmar: Amplifying Hate Speech?." Al Jazeera. June 14, 2014. http://www.aljazeera.com/.

Humanitarian Information Unit. U.S. Department of State. "Burma 2010 Election Results." accessed October 15, 2014. https://hiu.state.gov/Products/Burma_Elections2010and2012_2012Mar22_HIU_U553.pdf.

Info Security. "Myanmar Surprises as Top Source of Malicious Internet Traffic." August 10, 2011. http://www.infosecurity-magazine.com/.

ITU-IMPACT. *2012 Report*. Accessed October 26, 2014. http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf.

————-. "Mission." Accessed October 26, 2014. http://www.impact-alliance.org/aboutus/mission-&-vision.html.

Latt, Sai. "Intolerance, Islam and the Internet in Burma." New Mandala. June 10, 2012. http://asiapacific.anu.edu.au/newmandala/.

Libicki, Martin. "Don't Buy the Cyberype: How to Prevent Cyberwars from Becoming Real Ones." *Foreign Affairs.* August 13, 2013.

Lonely Planet. "Burma/Myanmar." Accessed October 15, 2014. http://www.lonelyplanet.com/myanmar-burma/practical-information/money-costs.

Mezzofiore, Gianlucca. "Wirathu's 'Buddhist Woman Raped' Facebook Post Stokes Anti-Muslim Violence in Mandalay." *International Business Times.* July 2, 2014. http://www.ibtimes.co.uk/.

Mircrosoft. *Microsoft Security Intelligence Report.* 2014.

NationMaster. Accessed October 20, 2014. http://www.nationmaster.com/country-info/profiles/Burma/Media/All-stats.

Oxford Business Group. "Myanmar: Internet Conundrum." April 26, 2013. http://www.oxfordbusinessgroup.com/.

Reporters Without Borders. "Press Freedom Index 2010." Accessed October 25, 2014. http://en.rsf.org/press-freedom-index-2010,1034.html.

Silk Road Drugs. "Silkroad." Accessed October 28, 2014. http://silkroaddrugs.org/silkroad/.

Stratfor Global Intelligence. "Myanmar: The United Wa State Army's Uncertain Future." July 22, 2013. http://www.stratfor.com/.

Tharoor, Ishaan. "Why Al-Qaeda is Opening a New Wing in South Asia." *The Washington Post.* September 3, 2014.

The World Bank. Accessed October 11, 2014. http://data.worldbank.org.

United Nations Office on Drugs and Crime. “Myanmar and UNODC Sign Landmark Agreement to Strengthen the Rule of Law and Counter Crime and Drug Threats.” August 18, 2014. https://www.unodc.org/southeastasiaandpacific/en/myanmar.

————-. *The Use of the Internet for Terrorist Purposes*. 2012. http://www.unodc.org/documents.

U.S. State Department. “U.S. Engagement in the 2014 ASEAN Regional Forum.” August 10, 2014. http://www.state.gov/r/pa/prs/ps/2014/230479.htm.

Walsh, Dean. “A Beginner's Guide to Exploring the Darknet.” Accessed October 24, 2014. http://electronician.hubpages.com.

Weimann, Gabriel. *How Modern Terrorism Uses the Internet*. U.S. Institute of Peace. March 2004. http://www.usip.org/sites/default/files/sr116.pdf.

Wong, Chun Han and Hatani, Shibani. “Telenor and Qatar Telecom Win Myanmar Licenses.” *The Wall Street Journal.* June 27, 2013. http://online.wsj.com/.